Ramanujan グラフと正則 LDPC 符号

平松 豊一 (法政大学工)　斎藤 正顕 (法政大学工)

はじめに

良いグラフの代表として Ramanujan グラフ (R-グラフ) G,
シャノン限界に近い良い符号の代表として LDPC 符号 C

の G と C がある. G から C を構成する歴史：

$$G \to C$$

I. R-グラフの構成の歴史

1) L-P-S (1986),　G.A. Margulis (1988)

2) A.K. Pizer (1990)

3) W.C. Li (1992)

4) P.E. Gunnells (2005)

II. LDPC 符号の構成の歴史

1) R.G. Gallager (1962) ··· 学位論文

2) R.M. Tanner (1981) ··· (一般化とグラフによる表現：ターナーグラフ)

3) D.J.C. MacKay (1995) ··· 再発見

III. $G \to C$ の歴史

1) G.A. Margulis (1982)

2) J. Rosenthal - P.O. Vontobel (2000)

I. R-グラフの構成の歴史

1.1 R-グラフとその性質

$G=(V,E)$: 連結な無向グラフ, 単純, k-正則 $(k \geqq 2)$
$V \ni v, w$ に対し, $v \sim w$ を定義する.
$f : V \to \mathbb{C}$,
$S_V = \{f\}$, $\{e_v : v \in V\}$: 標準基底

$$e_v(v)=1,\ e_v(w)=0,\ (w \neq v)$$

$A_G : S_V \to S_V$ 1 次変換, *i.e.*,

$$(A_G f)(v) = \sum_{w \sim v} f(w)$$

隣接作用素 (adjacency operator)
$\Lambda_G = \{A_G$ の固有値$\}$: G のスペクトル

A_G は基底 $\{e_v\}$ 上実対称行列だから, $\Lambda_G \subset \mathbb{R}$.
(1) $\Lambda_G \subset [-k, k]$,
(2) $m(k)=1$.

Definition 1 G : Ramanujan とは, Λ_G の $|\lambda| \neq k$ なるすべての元が, $|\lambda| \leqq 2\sqrt{k-1}$ をみたすとき.

リーマンのゼータ関数 $\zeta(s)$ がオイラー積

$$\zeta(s) = \prod_p \left(1-p^{-s}\right)^{-1}$$

をもつことの類似から, グラフ G のゼータ関数を定義する.

G : k-正則, 単純
閉路 $x_0, x_1, \ldots, x_n = x_0$ は $x_{i-1} \neq x_{i+1}$ ($i = 1, 2, \ldots, n$) のとき reduced という. 閉路 $x = (x_0, x_1, \ldots, x_n)$ に対し, x を k 個並べて作った閉路を

$$x^k = (x_0, x_1, \ldots, x_n, \ldots, x_0, x_1, \ldots, x_n)$$

とおく. 閉路 x は他の閉路 x' で, $x = (x')^k$ $(k \geqq 2)$ と表されないとき prime という. また, 2 つの閉路

$$x = (x_0, \ldots, x_n), \quad y = (y_0, \ldots, y_n)$$

は, $y_t \equiv x_{t+d} \pmod{n}$ for each t and some fixed d となるとき, 互いに equivalent であるという.
以上のもとで, G の伊原-砂田のゼータ関数

$$Z(s) = \prod_C \left(1 - \frac{1}{(k-1)^{s \cdot \ell(C)}}\right)^{-1},$$

$\prod_C$ は G 内の prime reduced な閉路の同値類 C 上の積, $\ell(C)$ は C の長さを表す.

Theorem 1.1 (砂田) $0 < \mathrm{Re}\, s < 1$ 内の $Z(s)$ の極がすべて $\mathrm{Re}\, s = \dfrac{1}{2}$ 上にあるための必十条件は, G が Ramanujan であることである.

これは, $Z(s)$ に関するリーマン予想の類似と考えられる. R-グラフの無限の世界での有用性がここにある.

1.2 R-グラフの構成

1) A. Lubotzky, R. Phillips and P. Sarnak : 1986, 1988 ([1])

$\cdots$ 隣接行列 A_G の固有値 = ある種の保型形式上の Hecke 作用素の固有値.

2) G.A. Margulis : 1988 $\cdots$ J. of Prob. of Inf. Transmission (vol. **24**)

3) A.K. Pizer : 1990 ([2])

4) W.C. Li : 1992 ([3])

5) P.E. Gunnells : 2005 ([4]) $\cdots$ 初等的構成法

5) の構成法 : Ramanujan graphs from modular curves
H^+ : 複素上半平面
$\Gamma = \mathrm{PSL}_2(\mathbb{Z})$
$H^* = H^+ \cup \mathbb{Q} \cup \{\infty\}$
とおく. Γ は H^* 上に作用する. 無限グラフ $G(\infty) = (V, E)$ を次で定義する:
$V = H^* \setminus H^+$, $V \ni v, w$ に対し,

$$v \sim w \Longleftrightarrow \exists \gamma \in \Gamma, \quad \gamma \cdot 0 = v, \quad \gamma \cdot \infty = w.$$

Definition 2 $N \geqq 2$: integer, $\Gamma(N) \subset \mathrm{PSL}_2(\mathbb{Z})$ に対し,

$$G(N) = \Gamma(N) \setminus G(\infty) \quad \text{(as quotient)}$$

とグラフ $G(N)$ を定義する.

$G(N)$ は具体的には次のように述べられる :

$$V(N) = \left\{(a,b) \in (\mathbb{Z}/N\mathbb{Z})^2 - (0,0) \,:\, (a,b,N) = 1\right\} / \{\pm 1\}$$
$$E(N) \ni ((a,b),(c,d)) \in V(N) \times V(N), \quad ad - bc = \pm 1$$

とするとき, $$G(N) \cong (V(N), E(N)).$$

Theorem 1.2 p : odd prime のとき, $G(p)$ は Ramanujan グラフとなる.

II. LDPC 符号の構成の歴史

2.1 LDPC 符号入門

Definition 3 パラメータ (n, i, j) をもつ低密度パリティ検査 (LDPC) 符号とは, 符号長が n で, 各行に j 個の 1 と各列に i 個の 1 をもつパリティ検査行列 H により定義される符号のこと.

m 行 n 列 $(m > n-k)$ の広義の検査行列 H のどの列のハミング重みも ω_c であり, どの行のハミング重みも ω_r であり, $\omega_c \ll m(< n)$ のとき, 検査行列 H によって定義される線形符号を正則 LDPC 符号という. このとき,

$$\frac{\omega_c}{\omega_r} = \frac{m}{n} \quad : \quad R = \frac{k}{n} \geqq 1 - \frac{\omega_c}{\omega_r}.$$

これに反し, 各行各列の重みが一定でない検査行列から得られる符号を非正則 LDPC 符号という.

符号長 n が十分大きい LDPC 符号は, Shannon 限界 に迫る復号性能を有する強力な誤り訂正符号であることが知られている.

R.G. Gallager $\cdots$ MIT 学位論文 (1962) [5]

この結果は, sum-product 復号法が当時の回路実装技術に不向きであったため, 約 30 年間埋もれていた後,

D.J.C. Mackay (1995), [7]

によって再発見された.

LDPC 符号を定義するもう一つの方法, 即ち 2 部グラフによる方法がある (両者は等価):

R.M. Tanner (1981), [6]

2 部グラフとは, ノードが 2 種類のグループに分かれ, 同じグループに属する 2 つの異なるノードの間には枝のない無向グラフのことである. このグラフに対して 2 元線形符号が一つ定まる. この符号を定義する 2 部グラフは Tanner グラフと呼ばれる.

Example 1 右図の 2 部グラフで, 記号 $c_1, \ldots, c_5$ は符号語のシンボルを表し, 0 または 1 の値をとる. 左端のチェックノードは, c_1, c_2, c_3 に接続しているが, これは

$$c_1 + c_2 + c_3 = 0 \pmod 2$$

という拘束条件を表している. これをパリティ検査条件という. 他の 2 つのチェックノードもそれぞれ次のパリティ検査条件を表している:

$$c_2 + c_3 + c_4 = 0, \quad c_3 + c_4 + c_5 = 0 \pmod 2.$$

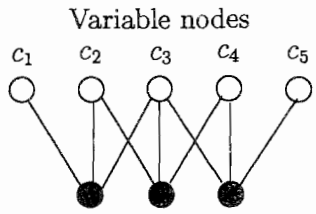


図 1

そして, これらの条件をみたす 2 元ベクトル

$$(c_1, c_2, \ldots, c_5)$$

の全体が図 1 の 2 部グラフから定義される符号となる:

$$\{(00000), (11011), (10110), (01101)\}.$$

LDPC 符号は疎な 2 部グラフから定義される符号である. ここで疎なグラフとはノード数に対して枝数が "非常に少ない" グラフのことである ("非常に少ない" の明確な定義はまだない).

III. $G \to C$ の歴史

3.1 G.A. Margulis (1978, 投稿年), [8] (1982)

$\cdots$ 先駆的研究

G : 有限群,

$A \subset G$: subset, $A^{-1} = A$

のとき, Cayley グラフ $X(G, A)$ とは, $E = G$, $G \ni g, h$ に対し, $g \sim h \Longleftrightarrow \exists a \in A$, $h = ga$ のときと定義する. $X(G, A)$ は, k-正則無向グラフである. ここで, $k = |A|$ とする. さて,

p : 奇素数,

$G = \mathrm{SL}_2(\mathbb{F}_p)$, $\quad |G| = p^3 - p$,

$$A = \left\{ a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, a^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, b^{-1} = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \right\},$$

とするとき,

Theorem 3.1 (Margulis) Cayley グラフ $X(G, A)$ は, $|E| = p^3 - p$ の 4-正則グラフで, その内周 (girth) c は

$$c \geqq 2 \log_\alpha \frac{p}{2} - 1, \quad \alpha = 1 + \sqrt{2}$$

をみたす. この $X(G, A)$ が R-グラフであることは後でわかる (1988).

この $X(G, A)$ から, $(2(p^3 - p), 3, 6)$-正則 LDPC 符号を次の様に構成する:

変数ノードとして, G の 2 つのコピー G, $\tilde{G}$ をチェックノードとして G をとる. 変数ノード $G \ni g$ に対し, チェックノードの元

$$ga^2, \quad gaba^{-1}, \quad gb$$

を接続し, $\tilde{g} \in \tilde{G}$ に対しては,

$$\tilde{g}a^{-2}, \quad \tilde{g}ab^{-1}a^{-1}, \quad \tilde{g}b^{-1}$$

を接続する. また, $\{a, a^{-1}, b, b^{-1}\}$ に関する最小の長さ c の関係式があったとき,

$$\{a^2, a^{-2}, aba^{-1}, ab^{-1}a^{-1}, b, b^{-1}\}$$

は, 長さが $\frac{c}{2}-1$ より小さい関係式をもつ.

Theorem 3.2 上で得た 2 部グラフは, $(2(p^3-p), 3, 6)$- 正則 LDPC 符号を構成し, 内周 c は

$$c \geqq 2\log_\alpha \frac{p}{2} - 1, \quad \alpha = 1+\sqrt{2}$$

をみたす.

3.2 J.Rosenthal-P.O.Vontobel (2000), [10]

L-P-S の Ramanujan グラフの構成法を利用し, それから正則 LDPC 符号を構成する.

$G' = \mathrm{GL}_2(\mathbb{F}_q)$,

$D = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} : x \in \mathbb{F}_q^\times \right\} : G'$ の normal subgroup,

$G = \mathrm{PGL}_2(\mathbb{F}_q) = G'/D$,

とする. $\#G = q^3 - q$ である. G の元は, 次で構成されている:

1) $\begin{pmatrix} 1 & b \\ c & d \end{pmatrix}$, $d \neq bc$, b, c : 任意 ... $q^2(q-1)$ 個

2) $\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix}$, $c \neq 0$, d : 任意 ... $q(q-1)$ 個

以下, q : 奇素数とする. $a \in \mathrm{GL}_2(\mathbb{F}_q)$, $x \in \mathbb{F}_q^\times$ に対し

$$\left(\frac{\det(xa)}{q}\right) = \left(\frac{\det(a)}{q}\right)$$

が成立する. このとき,

$$\varphi : G \ni aD \longmapsto \left(\frac{\det(a)}{q}\right) \in \{1, -1\}$$

なる φ は well-defined な homomorphism を与える.

Remark 1 $\varphi^{-1}(1) = \mathrm{PSL}_2(\mathbb{F}_q)$.

p, q：互いに異なる素数, $\equiv 1 \pmod 4$ とする.

$$p = a_0^2 + a_1^2 + a_2^2 + a_3^2 \tag{1}$$

は $p+1$ 個の解をもつ. $a_0 > 0$：odd, a_i $(i = 1, 2, 3)$：even (Jacobi). ここで, $i \in \mathbb{F}_q^\times$, $i^2 = -1$ なる i をとり,

$$A = \left\{ \begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix} \mid (a_0, a_1, a_2, a_3) : (1) \text{ の解} \right\}$$

とおく. $A^{-1} = A$ で, $a \in A$ に対し, $\det(a) = p$ となる.

$$X^{p,q} = X(G, A) : \text{Cayley グラフ}$$

Theorem 3.3 $p, q \equiv 1 \pmod 4$：互いに異なる素数, $\left(\frac{p}{q}\right) = -1$ のとき, $X^{p,q}$ は $q^3 - q$ 頂点をもつ 2 部グラフ, Ramanujan グラフで内周 c は

$$c \geqq 4 \log_p q - \log_p 4$$

をみたす.

次に, $p = 5$, $q = 17$ のとき $(n = q^3 - q = 4896)$ に, $X^{5,17}$ から $(4896, 3, 6)$-正則 LDPC 符号を構成する： $i = 4$, $i^2 = -1$ in $\mathbb{F}_{17}$,

$$5 = a_0^2 + a_1^2 + a_2^2 + a_3^2$$

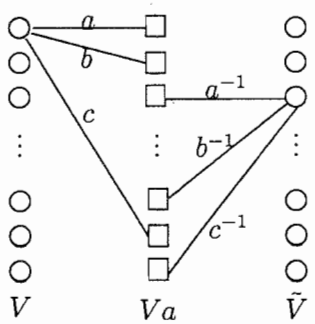
は $p + 1 = 6$ 個の解をもつ：

$$(1, \pm 2, 0, 0), \quad (1, 0, \pm 2, 0), \quad (1, 0, 0, \pm 2).$$

$$A = \left\{ a^{\pm 1} = \begin{pmatrix} 1 \pm 8 & 0 \\ 0 & 1 \mp 8 \end{pmatrix}, \quad b^{\pm 1} = \begin{pmatrix} 1 & \pm 2 \\ \mp 2 & 1 \end{pmatrix}, \quad c^{\pm 1} = \begin{pmatrix} 1 & \pm 8 \\ \pm 8 & 1 \end{pmatrix} \right\}$$

A の各元の $\det \equiv 5 \pmod{17}$ である. Cayley グラフ $X^{5,17}$ は 2 部グラフの構造を持つ. そして, これから次のように LDPC 符号が作られる.

変数ノードとして $\mathrm{PSL}_2(\mathbb{F}_{17})$ の 2 つのコピー $V, \tilde{V}$　チェックノードとして, $\mathrm{PSL}_2(\mathbb{F}_{17})$ の right coset $Va \subset \mathrm{PGL}_2(\mathbb{F}_{17})$ とする. $v \in V$ に va, vb, vc を, $v \in \tilde{V}$ に $\tilde{v}a^{-1}, \tilde{v}b^{-1}, \tilde{v}c^{-1}$ を夫々接続させる. code bit は V と $\tilde{V}$ で表される. この結果, 長さ $n = 4896$, parity-check 方程式の数 $m = 2448$ の $(3, 6)$-正則 LDPC 符号が得られた (Ramanujan-Margulis 符号ともいう).



Remark 2 (シャノン限界 (通信路符号化定理) : 1948)

R1 通信路を最も有効に利用したと云う意味で, 伝達情報量の最大値を '通信路容量' という.

R2 シャノンの通信路符号化定理 : q 元通信路の通信路容量 $K \neq 0$ とする. $K > R$ なる任意の正数 R と任意の自然数 n に対して, 符号化率 $\geqq R$, 正しく復号されない確率 P_e が次式で与えられる符号長 n の q 元ブロック符号が 存在する :

$$P_e \leqq c_1 2^{-c_2 n},$$

ここで, c_1, c_2 は通信路と R のみによって決まる正数である.

参考文献

[1] A. Lubotzky, R. Phillips and P. Sarnak : Ramanujan graphs, Combinatorica **8** (1988), no.3, 261-277.

[2] A. Pizer : Ramanujan graphs and Hecke operators, Bulletin of the A.M.S., **23** (1990), 127-137.

[3] W. Li : Character sums and abelian Ramanujan graphs, J. Number Theory **41** (1992), no.2, 199-217.

[4] P.E. Gunnells : Some elementary Ramanujan graphs, Geometriae Dedicata **112** (2005), 51-63.

[5] R. Gallager : Low-density parity-check codes, IRE Trans. Information Theory, IT-**8** (1962), 21-28.

[6] R.M. Tanner : A recursive approach to low complexity codes, IEEE Trans. Information Theory, IT-**27** (1981), 533-547.

[7] D. MacKay : Good error correcting codes based on very sparse matrices, IEEE Trans. Information Theory, IT-**45** (1999), 399-431.

[8] G.A. Margulis : Explicit constructions of graphs without short cycles and low density codes, Combinatorica **2** (1982), no.1, 71-78.

[9] M. Sipser and D.A. Speilman : Expander codes, IEEE Trans. Information Theory, IT-**42** (1996), 1710-1722.

[10] J. Rosenthal and P.O. Vontobel : Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis, In Proc. 38 th Annual Allerton Confer. on Comm., Control and Computing (2000), 248-257.